

# CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

As noted by CSU ICSUAM 3101.02, Campus Administration of Systemwide Cash Management Policy, it is the policy of the CSU that systemwide cash management policies be implemented in a manner that meets the internal control objectives and documentation retention requirements of the University. Certain basic internal control principles must be adhered to in regards to collecting and accounting for cash and cash equivalents. These basic principles are articulated below:

## Key Objectives:

### 1. Accountability

- a. **Ensures that CSUF employees who process and/or handle cash and cash equivalents can be held responsible in fulfilling their duties.**
- b. **Accountability is present when the following three (3) areas are addressed:**
  - i. Knowledge of who has or had access to, and why he/she has or had access to, cash and cash equivalents;
  - ii. Knowledge of where cash or cash equivalent assets are at all times; and
  - iii. Knowledge of what transpired from the beginning of a cash handling process to the conclusion of the process

### 2. Separation of Duties

- Ensures that two (2) or more qualified and authorized persons are involved in the key, most sensitive activities related to the collection, handling, depositing, and accounting processes.

### 3. Security (Physical and Information)

- Ensures that employees involved in the handling of cash and cash equivalents are, at all times, protected from physical harm.
- Ensures that cash and cash equivalents are at all times, protected from loss or misuse.
- Ensures that technology resources (i.e. hardware and confidential payment information) are at all times protected from loss, corruption or compromise to confidentiality.

### 4. Reconciliation of Accounts

- Provides assurance that cash and cash equivalents collected and reported as deposits are deposited accurately and timely into authorized CSUF bank accounts.
- Provides assurance that general ledger recordings/transactions are recorded accurately and timely.

### 5. Authorized Bank Accounts

- Provides assurance that there are no unauthorized bank accounts with local banks that use the campus name, address, and Federal identification number (FEIN).

# CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

California State University, Fullerton  
CASH MANAGEMENT POLICY

<u>Table of Contents</u>	<u>Page</u>
<a href="#">References</a>	4
I. <a href="#">Introduction</a>	5
A. Key Objectives	5
1. Accountability	5
2. Separation of Duties	5
3. Security (Physical and Information)	5
4. Reconciliation of Accounts	6
II. <a href="#">Definitions</a>	6
III. <a href="#">Roles and Responsibilities</a>	8
A. Office of the CSU Chancellor	8
B. Campus Administration	9
IV. <a href="#">Conditions for Employment in a Cash Handling Environment</a>	10
V. <a href="#">Managing CSUF Bank Accounts</a>	10
A. Bank or Other Financial Institution Accounts Maintained by Related Entities	11
VI. <a href="#">Establishing Credit and Debit Card Merchants</a>	12
VII. <a href="#">Payment Types</a>	13
A. Currency and Coin	13
B. Checks and Cash Equivalents	14
VIII. <a href="#">Payment Channels</a>	15
A. General Cashiering Policies for Receiving and Recording Cash and Cash Equivalents	15
B. Receiving and Recording Cash and Cash Equivalents	16
C. Point of Sale Equipment - Debit and Credit Card Processing	18
D. Point of Purchase (POP) & Back Office Conversion (BOC) ACH Requirements	18
E. Sale of Admission or Event Tickets	18
F. Credit/Debit Card Batch Processing (University of Extended Education ONLY)	19
G. Telephone	19
1. Credit/Debit Card Batch Processing (University of Extended Education ONLY)	19
H. Prohibition on Payment with Credit/Debit Card Via Fax Transmissions	20
I. Payment with Credit-Debit Cards via the Internet	20
1. Information Security	20
2. Credit/Debit Card Gateway	20
3. WEB ACH Transactions	21
IX. <a href="#">Physical Security</a>	21
X. <a href="#">Recording Deposits to the General Ledger</a>	23
XI. <a href="#">Returned Item Processing</a>	24

# CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

A.	Cash Equivalents (non-coin & currency) and Checks	24
B.	ACH Debit Transactions	24
C.	Credit/Debit Card Chargebacks	25
XII.	<a href="#">Contracting With Third Party Relationships to Process Cash and Cash Equivalents (Includes Lockbox Services)</a>	26
XIII.	<a href="#">Petty Cash and Change Funds</a>	27
Appendix A:	<a href="#">General Information</a>	30
	A. Credit and Debit Card Information	30
	B. Detecting Counterfeit Money	30
	C. Reason Codes for why Payment Types may be Returned	30
Appendix B:	<a href="#">PCI-DSS Data Security</a>	32
Appendix C:	<a href="#">ICSUAM 3101.02 Annual Compliance Checklist</a>	34

# CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

## REFERENCES

### California State University System

California State University, System (CSU) Chancellor Office ICSUAMs:

<http://www.calstate.edu/icsuam/sections/3000/>

- 3101.02 - Campus Administration of Systemwide Cash Management Policy
- 3102.01 - Sensitive Positions and Cash Handling
- 3102.02 - Segregation of Cash Handling Duties
- 3102.03 - Acceptance of Cash and Cash Equivalents
- 3102.04 - Physical Protection of Cash and Cash Equivalents
- 3102.05 - Debit/Credit Card Payment Policy
- 3102.06 - Returned Items
- 3102.08 - Recording Deposits to the General Ledger
- 3102.09 - Bank Reconciliations
- 3102.10 - Change Funds
- 3102.11 - Deposits and Transfers to the Bank
- 3103.11 - Petty Cash

CSU Chancellor's Office Resource Management, Cashiering Policies of the California State University

[http://www.sfsu.edu/~bursar/staff/cash\\_guidelines/CSU%20Cashiering%20and%20Cash%20Handling%20Guidelines.pdf](http://www.sfsu.edu/~bursar/staff/cash_guidelines/CSU%20Cashiering%20and%20Cash%20Handling%20Guidelines.pdf)

CSUF Petty Cash & Change Funds Policy, <http://finance.fullerton.edu/Controller/Accounting/PettyCash/>

### Federal and State

California Civil Code §§1798.29 and 1798.82 (SB [1386](#), *Personal Information, Privacy*)

Internal Revenue Service (IRS):

- Form 8300, Report of Cash Payments over \$10,000 Received in a Trade or Business  
[http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Form-8300-and-Reporting-Cash-Payments-of-Over-\\$10,000](http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Form-8300-and-Reporting-Cash-Payments-of-Over-$10,000)
- Publication 1544, Reporting Cash Payments of over \$10,000

State of California Information Practice Act ([Senate Bill 1386](#)), Peace. Personal information: Privacy

United States Secret Service, *Know your Money Guidelines*,

[http://www.secretservice.gov/know\\_your\\_money.shtml](http://www.secretservice.gov/know_your_money.shtml)

### Other Resources

Purchase Card Industry (PCI) Data Security Standards compliance requirements.

[http://usa.visa.com/download/business/accepting\\_visa/ops\\_risk\\_management/cisp\\_PCI\\_Data\\_Security\\_Standard.pdf?it=ill/busines/accepting\\_visa/ops\\_risk\\_management/cisp.html|PCI\\_Data%Security%Standard](http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf?it=ill/busines/accepting_visa/ops_risk_management/cisp.html|PCI_Data%Security%Standard)

# CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

## I. INTRODUCTION

CSU ICSUAM 3101.02, Campus Administration of Systemwide Cash Management Policy, states it is the policy of the CSU that systemwide cash management policies be implemented in a manner that meets the internal control objectives and documentation retention requirements of the University. This document establishes the California State University, Fullerton (“CSUF”) policies and procedures related to handling and processing cash and cash equivalents. Its purpose is to ensure that important CSUF assets are protected, accurately processed, and properly reported.

Policy statements are specifically identified and numbered as Policies in this document. Procedural statements are included, but do not have specific numbers. **All policy statements are indicated in bold type.**

Certain basic internal control principles must be adhered to in regards to collecting and accounting for cash and cash equivalents. These basic principles are articulated below:

### A. Key Objectives of this document:

#### 1. Accountability

- a. Ensures that CSUF employees who process and/or handle cash and cash equivalents can be held responsible for fulfilling their duties.
- b. Accountability is present when the following three (3) areas are addressed:
  - i. Knowledge of who has or had access to, and why he/she has or had access to cash and cash equivalents;
  - ii. Knowledge of where cash or cash equivalent assets are at all times; and
  - iii. Knowledge of what transpired from the beginning of a cash handling process to the conclusion of the process.

#### 2. Separation of Duties

- a. Ensures that two (2) or more qualified and authorized persons are involved in the most sensitive activities related to the collection, handling, depositing, and accounting processes.

#### 3. Security (Physical and Information)

- a. Ensures that employees involved in the handling of cash and cash equivalents are at all times protected from physical harm.
- b. Ensures that cash and cash equivalents are at all times protected from loss or misuse.
- c. Ensures that technology resources (i.e. hardware and confidential payment information) are at all times protected from loss, corruption or compromise to confidentiality.

#### 4. Reconciliation of Accounts

- a. Provides assurance that cash and cash equivalents collected and reported as deposits are deposited accurately and timely into authorized CSUF bank accounts.

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

- b. Provides assurance that general ledger recordings/transactions are recorded timely and accurate. Monthly reconciliation of deposit records must be performed to ensure that all deposits are deposited into a University depository account and properly recorded on the general ledger in an accurate and timely manner.

## II. DEFINITIONS

For purposes of this document:

- A. The term “Campus” is defined as a CSUF Campus or other official CSUF location. The abbreviation “CSUF” is defined as California State University, Fullerton.
- B. Cash Handling Units are defined generally as follows for assignment of responsibility:
  1. Main Cashiering Station  
A campus operating unit from which collections are deposited directly to a CSUF bank account. The Fullerton location is in UH-180 and the Irvine location is in Room 127.
  2. Satellite Cashiering Station  
A Campus operating unit which typically perform cashiering activities as a primary function and operates cash handling equipment. Satellite Cashiering Stations may deposit directly to an approved depository bank accounts on behalf of Main Cashiering Stations.
  3. Cash Handling Department  
A campus operating unit that typically collects cash or cash equivalents and deposits to either a Main Cashiering Station or a Satellite Cashiering Station.
- C. Types of Payments Received -- Cash and Cash Equivalents:

Additional information defining each payment type can be found in Appendix A.

1. Currency and Coin (“Cash”)  
Currency and Coin are the most liquid of assets and must be immediately, and at all times, protected against loss or misuse.
2. Cash Equivalents (Money Orders, Travelers Cheques, Cashiers Checks, Certified Checks)
  - a. Money Orders  
  
Money Orders are preprinted fixed-amount checks issued by a bank or other financial institution allowing the individual named on the order to receive a specified amount of cash on demand.
  - b. Travelers Cheques  
  
Travelers Cheques are preprinted, fixed-amount checks designed to allow the person signing to make an unconditional payment to someone else as a result of having paid the issuer (usually a bank) for that privilege.
  - c. Cashier’s Check (also known as Official Check)

The term “Cashier’s Check” means any check which is:

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

- drawn on a depository institution;
- signed by an officer or employee of such depository institution; and
- a direct obligation of the depository institution.

### d. Certified Check

The term “Certified Check” means any check for which a depository institution certifies that:

- the signature on the check is genuine; and
- depository institution has set aside funds equal to the amount of the check and to only pay that check.

### 3. Check

The term “check” (including those instruments issued and commonly called warrants by the State of California) means any negotiable demand draft drawn on or payable through a United States office of a depository institution that is a qualified member of the United States’ Federal Reserve Bank.

### 4. Automated Clearing House Payments (ACH)

ACH transactions are electronic payment instructions to either debit or credit a deposit account at a participating Receiving Depository Financial Institution (“RDFI”).

### 5. Wire Transfer

Wire Transfers are non-recourse, electronic funds transfers moving value from one bank account to another bank account through bookkeeping entries typically processed over the United States’ Federal Reserve Bank’s electronic network.

### 6. Credit and Debit Card

Credit Cards, issued by commercial banks and financial institutions under the Visa and MasterCard brands and by independent companies, (American Express and Discover), permit CSUF clients to pay for services and goods by drawing against lines of credit granted by the card issuing banks/companies.

Signature-based Debit Cards, also issued by financial institutions under the Visa and MasterCard brands, permit CSUF clients to pay for services and goods by drawing against available funds resident in the payer’s checking or savings account at the time of the payment.

PIN-based Debit Cards, also issued by financial institutions, rely on connectivity to various Debit Card switching networks such as STAR, Interlink, NYCE, PULSE and several others. These cards permit CSUF clients to pay for services and goods by drawing against available funds resident in the payer’s checking or savings account at the time of the payment.

- D. Petty Cash funds are those established by Accounting Services & Financial Reporting and audited by the campus Director of Internal Audit for small expenditures when the use of regular purchasing procedures is not required. <http://finance.fullerton.edu/Controller/Accounting/PettyCash/>

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

- E. Change Funds are established by Accounting Services & Financial Reporting and audited by the campus Director of Internal Audit which is used to provide a constant amount of change, both in currency and coin at cash collection stations. <http://finance.fullerton.edu/Controller/Accounting/PettyCash/>
- F. Managing CSUF Bank Accounts

Financial Institution Account: Any domestic or foreign account (checking, savings, depository, brokerage, investment, custodial, asset management, petty cash, etc.) at an institution providing financial services to the University that:

- Carries the name or similarity of “California State University, Fullerton;” and/or
- Uses the University’s Tax Identification Number; and/or
- Records receipts or disbursements of University funds; and/or
- Holds financial assets for the University; and/or
- Processes financial transactions for the University

Tax Identification Number: The number used to identify the California State University, Fullerton for Federal and State tax matters. The Tax Identification Number may also be referred to as the Employer Identification Number (EIN) or Federal Employer Identification Number (FEIN).

University units: Schools and departments within the University, typically represented by a five digit numeric code in the Common Financial System (CFS).

### III. ROLES AND RESPONSIBILITIES

#### A. Office of the CSU Chancellor (“CSU CO”, “CO”, “Chancellor’s Office”)

1. The CSU’s Chief Financial Officer (CFO) shall develop and publish CSU system wide cash handling policies and procedures and provide general coordination and assistance to Campuses. The CFO shall:
  - a. Select the commercial banks into which funds of CSUF are deposited and from which such funds are disbursed,
  - b. Designate the name of the CSU to all bank accounts and assume direct ownership of such bank accounts, including time certificates of deposit, and to make withdrawals from or close such accounts,
  - c. Designate representatives of the CSU who may sign checks or other orders for the payment of money, including electronic transfers of funds (EFT), Credit/Debit cards, wire transfers and ACH transfers, and to approve the use of and direct banks to honor facsimile signatures,
  - d. Make arrangements for internet payment services, lockbox, electronic transfer of funds, escrow services, credit/debit card and other services to facilitate the collection or disbursement of funds, and
  - e. Open, make changes to, and close CSUF bank accounts.

These duties may be further delegated by the CFO to the Assistant Vice Chancellor-Financial Services and the Senior Director- Financing & Treasury or other Chancellor’s Office representatives, as appropriate.

2. The Chancellor’s Office Treasury Department (Treasury) is responsible for managing all relationships with organizations that provide banking and/or payment services to the CSU’s, opening, changing instruction to, and closing bank accounts when requested by authorized

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

Campus employees and authorized by the CFO or his/her delegates, maintaining an inventory of authorized CSU bank accounts and conducting periodic reviews of bank credit quality. See section V, Managing CSUF Bank Accounts, for additional information.

3. Chancellor's Office Treasury Department (Treasury) must approve the use of any third party that is in possession of CSU assets to process CSU cash, cash equivalents, checks and/or electronic entries.

### B. Campus Administration (California State University, Fullerton):

1. The Campus President is responsible for all Campus cash handling activities in accordance with the policies and procedures established in this document. The Campus President is also responsible for making requests to the campus CFO and his/her delegates to open, make changes to, or close bank accounts. The President may delegate the responsibility for all cash handling operations on the Campus to the Campus Chief Financial Officer (Campus CFO).
2. The Campus CFO or designee is responsible for implementing this policy on a Campus level and managing the process for granting all variances from these procedures when warranted by local circumstances. The person or persons properly authorized to sign checks, drafts, or other orders for the payment of money or approve/release electronic transfers of funds against CSUF financial institution accounts, provided that all such representatives are covered by a fidelity bond.

The Campus CFO or his/her designee must:

- a. Notify Treasury of monies deposited electronically to or disbursed electronically from any CSU commercial bank account only when an individual transaction is equal to or exceeds \$200,000.
- b. Notifications to Treasury need to be made one business day prior to the transaction's settlement date.
  - i. Electronic deposits and disbursements include, but are not limited to, Automated Clearing House (ACH) transactions, wire transactions, or direct bank-to-bank electronic settlements.
  - ii. The transaction amount in the notification can be actual or estimated.
  - iii. Notifications to Treasury can be made via SharePoint, email, telephone, or other Treasury approved method.
  - iv. In such cases where a campus contracts with third party vendors for the electronic collection or disbursement of funds, campuses are still responsible for delivering prompt and accurate notifications to Treasury.
  - v. Failure to comply with notification requirements may negatively impact systemwide cash positioning; consequently, Treasury may request a delay of disbursements.
  - vi. If an overdraft occurs due to untimely or no notification by a campus, any resulting overdraft penalties will be passed through to that campus.
  - vii. The transaction amount can be actual or estimated.
3. The University Controller and/or the Director (or Associate Director) of Student Financial Services (SFS) has the responsibility for the following:
  - a. Categorizing cash handling departments and individuals performing functions related to cash handling accounting.
  - b. Arranging for the preparation and implementation of operating procedures in accordance with this document.
  - c. Approving and documenting variances from these policies and procedures when warranted by local circumstances.

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

- d. Periodically reviewing the need for maintaining each of their bank accounts and subaccounts.
4. The University Controller and/or the Director (or Associate Director) of SFS is also responsible for the following:
- e. Serving as the central point of contact for implementing these policies and appropriate procedures on campus.
  - f. Reviewing and approving all proposed new or modified cash handling related applications, cash recording equipment, or methods of transporting cash.
  - g. Performing an annual documented review of compliance with these policies and procedures and reporting on the risks associated with each campus cash-handling department to the campus CFO.
  - h. Responsible for creating and or dismantling approved cashiering/sub-cashiering locations, stations, websites, third party processors, or any channel of accepting credit card payments.
  - i. Credit Card Acceptance Authority-The person properly authorized to act on requests concerning acceptance of commercial credit cards in payment of fees related to CSUF activities.
  - j. Act as the Credit Card Coordinator / Internet Payment Gateway. In this role, the individual serves as the:
    - i. Central point of contact for the establishment of new Campus credit card merchant accounts, with regard to set up with the merchant bank and Internet service provider if applicable. Ensures that such accounts are properly instituted from the perspective of both vendor management and internal accounting standpoint.
    - ii. Maintains institutional records of “merchants” operating on the campus, and to document equipment assigned to and services provided by each such merchant (merchant bank services and Internet payment gateway services).
    - iii. Ensures that all University units processing credit or debit card transactions receive ongoing training regarding the data security requirements for handling cardholder data and that such units are complying with the credit card data security requirements for their operating environment including completion of mandated data.
    - iv. Act as the reviewer of credit card and payment gateway charges and qualification performance and to address problems with merchants as they arise to ensure the most cost-effective use of services.

#### IV. CONDITIONS FOR EMPLOYMENT IN A CASH HANDLING ENVIRONMENT

Under ICSUAM 3102.01, Sensitive Positions and Cash Handling, campus management must determine that all employees with direct cash handling duties, including temporary, casual, and student employees, have the background and character to accept responsibility and accountability for handling CSUF cash and cash equivalents. *Employees with direct access to, or control over, cash, checks, other cash equivalents, credit cards, and/or credit card account information are considered to hold Sensitive Positions and are subject to background checks in accordance with HR Coded Memo 2005-10 and/or its successor policy. The only exception to this policy is for temporary cash handling activities (e.g., parking attendants, ticket sellers) which may not warrant background checks. Instead, mitigating supervisory review controls should be employed in such instances*

**Policy IV.1:** **In accordance with HR Coded Memo 2005-10, background checks are required for cashiers and other cash handlers defined as sensitive positions; new employees’ and student assistants’ employment should be considered provisional until such a background check is completed. Any felonies, misdemeanors, or judgments due to fraud related to cash (ICSUAM 3102.01), stocks, bonds or any other financial transactions should be addressed immediately.**

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

- Policy IV.2:** Each department supervisor is responsible for training of new employee of proper cashing procedures, all cash handling policies, and including processes for campus emergencies. The policies may vary based on multiples roles within the cashiering office and due to segregation of duties.
- Policy IV.3:** Each department supervisor is responsible for arranging the appropriate background and employment verifications when hiring employees into sensitive positions as defined by HR Coded Memo 200510. Before hiring a new cash-handling employee or finalizing a transfer into a sensitive position, the following must be completed:
- Employment history must be verified for all prospective employees.
  - Background checks, supported by fingerprinting to identify any prior criminal convictions must be completed.
  - Other procedures may be conducted as deemed necessary by the hiring manager in accordance Human Resources guidelines given the circumstances (e.g. credit checks).
- Policy IV.4:** Continuous bonding is an absolute condition for retaining cash handling responsibilities. If the cash handling employee's bonding cannot be maintained, the employee's cash handling responsibilities must be terminated. The requirements for bonding must be reviewed regularly for employees handling cash.
- Policy IV.5:** If any employee having cash handling responsibilities is convicted of a felony or any crime related to cash, that conviction must be reported to Campus Police and Human Resources.

### V. MANAGING CSUF BANK ACCOUNTS

- Policy V.1:** Pursuant to the Standing Orders of the Board of Trustees of the California State University and a Delegation of Authority concerning the "Deposit, control, investment, expenditure, and lending of funds," only the Office of the Chancellor has the authority to open, make changes to, or close official CSUF bank accounts. Related University auxiliary organizations' bank accounts are not subject to this requirement.
- Policy V.2:** The Campus President or the President's authorized designee (Campus CFO or designee) may recommend such requests noted in Policy V.1.

State of California Government Code Section 13401(b)(3) states that all levels of management of state agencies must be involved in assessing and strengthening the systems of internal accounting and administrative control to minimize fraud, errors abuse, and waste of government funds.

No individual or organization may open a bank account to transact business in the name of the University. All University business must be conducted under the auspices of an approved campus fiscal agency. Deposit of University Funds to a private bank account is considered prima facie evidence of embezzlement.

Accordingly, it is this institution's policy that all funds received by University related entities, including University departments, affiliated organizations, and student clubs and organizations, be deposited in accounts maintained by the University CFO, one of the University's recognized auxiliaries, or other banking institutions approved by the University CFO, as appropriate. Exceptions to this requirement are organizations (entities) that have separate legal status granted by the state/federal government (i.e., IRC §

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

501(c)(3), IRC § 501(c)(7), etc.). These organizations may open and maintain such accounts in accordance with their respective by-laws and by written consent of their governing bodies. The collection of funds, regardless of depository, must be conducted in a manner that facilitates proper cash control. All funds will be used in a manner consistent with relevant State, CSU, or campus policy.

**Policy V.3: Any bank account opened for University purposes but not established and authorized by the Office of the Chancellor must be immediately brought to the attention of the Campus CFO or designee and CSU CO Treasury Department (Treasury) for resolution.**

### **Bank or Other Financial Institution Accounts Maintained by Related Entities:**

Financial Institution accounts established and maintained for the purpose of student groups, alumni groups, employee-sponsored social events and other purposes not directly associated with University business do not normally constitute funds of the University. Accordingly, related entities and individuals who maintain such accounts may **not**:

- use the University's Tax Identification Number on such accounts;
- deposit funds made payable to, or intended for, the University, regardless of payee name, into such account;
- present themselves as University employees or agents of the University; or
- use the California State University, Fullerton name without approval from the Campus CFO or designee.

The State Administrative Manual (SAM section 8002.5) states,

*"Employees involved in activities which are not an integral part of State programs or operations must be involved only on their own time and without the use of State equipment or supplies. Any funds, which are collected or controlled by State employees for such non-State activities, are not to be accounted in the State Treasury. Non-State monies are to be collected, controlled, and expended in a manner that will prevent any implication that the State is a sponsor or participant in those activities."*

Exceptions for deposits made outside approved accounts, other than those with separate legal status, are possible for unusual and documented circumstances. The establishment of off-campus bank accounts by State employees for activities associated with any unit of the University is to be strictly monitored and controlled. Any requests for University related off-campus bank accounts must be submitted and approved by the University CFO or designee prior to the establishment of the account.

## VI. ESTABLISHING CREDIT AND DEBIT CARD MERCHANTS

CSUF campus departments may make a request to the Director (or Associate Director) of SFS to receive payment for goods and services by means of a Credit or Debit Card. CSUF campus departments are encouraged to perform a "needs" analysis regarding the acceptance of Credit or Debit Cards at any point of sale.

**Policy VI.1: The Director (or Associate Director) of SFS has the authority to accept or reject requests for Campus Merchant Card Services from campus departments. Final approval is by the University Controller.**

**Policy VI.2: Each Campus that accepts Debit and Credit Cards must develop its own rules and policies for the establishment of Credit and Debit Card Merchants (CSUF campus departments acting as "vendors" providing services or selling goods to the campus community [Campus Merchants]).**

When approving a department as a new Campus Merchant, the Director (or Associate Director) of SFS will:

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

- Determine whether the new Campus Merchant intends to accept Visa, MasterCard, American Express or Discover and whether it intends to accept both Credit and Debit Cards.
- Consider whether the new Campus Merchant is able to provide access to a telephone line or appropriate secured website that will permit automatic Credit and Debit Card processing by swiping the Credit or Debit card. Alternatively, the SFS Appropriate Administrator will determine the proper method of accepting Credit or Debit cards in the absence of a telephone line.
- Determine if the Campus Merchant intends to accept *Cardholder Present* Transactions and make certain that the Campus Merchant has a secure means of storing the signature verification provided by the buyer/payer at the point of sale or payment.
- Determine if the new Campus Merchant intends to accept *Cardholder Not Present* Transactions and make certain that the Campus Merchant has excellent record-keeping practices and can reassemble the transaction in the event of a dispute or a chargeback.
- Determine whether the proposed Campus Merchant understands and can comply with the Purchase Card Industry Data Security Standards (PCI-DSS) compliance requirements and assumption of liability for loss requirements (<http://www.pcisecuritystandards.org/index.htm>).
- Determine whether the proposed Campus Merchant understands the need to protect personal, sensitive information from disclosures and can meet the compliance of the California Information Practice Act (Senate Bill 1386) and similar regulatory requirements.
- Determine whether the proposed Campus Merchant can deposit directly into a CSUF bank account, or if the funds will be routed to a third party, and, if so, how long it will take for the funds to be deposited to an account in the name of and under the full control of CSUF. The campus may only choose third party handlers from an approved list of vendors, as provided by CSU CO Treasury Department.

### **Policy VI.3**

**All Campus Merchant Card accepting locations must use an approved CSUF Merchant Card processor under a University purchasing agreement. Such approved purchasing agreements ensure the most cost effectiveness and greatest level of service and compliance for the campus.**

### **Policy VI.4**

**Any CSUF department or unit wishing to process credit or debit cards (aka Campus Merchant Card accepting location) must adhere to the PCI-DSS as it applies to the unit's processing environment.**

**The classification of the environment will include such parameters as *Card Present* or *Card Not Present* transactions, consideration of whether cardholder data is collected, transmitted, or stored on University systems, and whether such systems are accessible from the internet. Merchants are required to provide a copy of their PCI-DSS Attestation of Compliance form. Depending upon the environment, the PCI-DSS may require additional testing of merchant systems. Merchants must perform the tests indicated for their environment. A discussion of these security standards and additional testing requirements is included in Appendix B PCI-DSS Data Security.**

**The above is coordinated with the campus Information Security Officer by the Director (or Associate Director) of Student Financial Services. The Information Security Officer will perform an annual review and testing of all locations, including online payment site to PCI-DSS compliance.**

# CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

**Policy VI.5** Any department or unit acquiring a payment application from a 3rd party vendor which will be operated on a University system and which will collect, store, or transmit cardholder data must only acquire such applications that are certified as complying with Payment Application Data Security Standards (PA-DSS, may also be referred to as PABP). While having a PA-DSS compliant application does not in and of itself ensure a merchant is PCI compliant, it will facilitate the process. Accordingly, any unit developing their own payment application that will operate on a University system should look to the PA-DSS standards for guidance on how to design the application so that it will not prevent the merchant from being PCI compliant.

The above PA-DSS standards compliance is coordinated with the campus Information Security Officer by the Director (or Associate Director) of Student Financial Services.

## VII. PAYMENT TYPES -Types of Payments Received (Cash, Cash Equivalents, and Checks)

### A. Currency and Coin (“Cash”)

Currency and Coin are the most liquid of assets and must be immediately, and at all times, protected against loss. The physical security of Currency and Coin is crucial (See Physical Security, Section IX, for cash security best practices). Financial recording of Currency and Coin immediately upon receipt is an essential function that ensures employee accountability. Employee accountability requires that the manager and appropriate individuals know **who** has authorized access to an asset, **why** he/she has access to the asset, **where** an asset is at all times, and **what** has occurred to the asset from the beginning to the end of the cash-handling transaction cycle.

The following are unique requirements associated with Cash:

**Policy VIIA.1:** **Large Dollar Transaction Reporting Requirements: Each Campus must comply with Federal and State Laws and Regulatory requirements associated with transactions involving currency and coin.**

The Internal Revenue Service (IRS) under the Bank Secrecy Act (Internal Revenue Manual, 4.26) requires tax-exempt education organizations to report cash transactions exceeding \$10,000 (single transaction or accumulated by multiple transactions) received in the course of a trade or business, even if the income is not subject to the unrelated business income tax. The reporting requirement applies **only** to cash transactions. When CSUF receives a cash transaction from an individual for more than \$10,000 the cashiering supervisor/manger must complete and file IRS [Form 8300, Report of Cash Payments over \\$10,000 Received in Trade or Business](#), with the IRS on or before the 15<sup>th</sup> day after the date of the cash transaction, or two or more related business transactions that occur within a 15-day period. IRS Publication 1544, [Reporting Cash Payments of over \\$10,000](#), contains additional information of the filing requirements.

1. A Campus Merchant Card or cashier location that observes a transaction or a series of transactions where both the following occur should contact the University police, University Controller and other appropriate Campus and CSU Systemwide units to ensure compliance with FBAR (Foreign Banking and Reporting) under the U.S. Bank Secrecy Act.
  - a. A transaction or series of transactions that involves funds or other assets of \$2,000 or more, AND
  - b. The unit knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part) falls into one or more of the following categories:

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

- It involves funds derived from illegal activity, or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any federal law or regulation, or to avoid any transaction reporting requirement under federal law or regulation; or
- Is designed to evade any regulations; or
- Has no business or apparent lawful purpose, or is not the sort in which the particular customer would normally be expected to engage, and the unit knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- Involves use of the money services business to facilitate criminal activity

**Policy VIIA.2: A Campus Merchant Card accepting or cashier location may accept only United States Dollar based coin and currency. No CSUF department or unit may accept non-U.S. currency as payment.**

- B. Checks and Cash Equivalents (including Money Orders, Travelers Cheques and Certified Checks - see Appendix A for more information regarding these instruments).

The term “check” (including those instruments issued and commonly called warrants by the State of California) means any negotiable demand draft drawn on or payable through a United States office of a depository institution that is a qualified member of the United States’ Federal Reserve Bank.

**Policy VIIB.1: All checks must be payable to “California State University, Fullerton”, CSUF or reasonable variation on such names and must include:**

- a. Dating no earlier than 180 days prior to the day of acceptance (unless a shorter time period is clearly marked on the face of the check) and no later than the day of acceptance**
- b. Legible and consistent amount, both numeric and written**
- c. Proper account holder signature.**

**Policy VIIB.2: Checks and Cash Equivalents stamped or otherwise identified as “Payable/Paid in Full” are not to be accepted. The check must be returned to the presenter, and must not be deposited.**

**Policy VIIB.3: All campus documents or communications that request payments be made to CSUF must inform all payers that their payments must be made payable to “California State University, Fullerton”, CSUF or reasonable variations on such names.**

### VIII. PAYMENT CHANNELS

This Section covers policies for receiving and recording cash and cash equivalents presented in person or through common mail carrier. The acceptance of cash and cash equivalents is governed by following CSU Chancellor’s Office ICSUAMs:

- 3102.02 - Segregation of Cash Handling Duties
- 3102.03 - Acceptance of Cash and Cash Equivalents
- 3102.05 - Debit/Credit Payment Policy.

- A. General Cashiering Policies for Receiving and Recording Cash and Cash Equivalents

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

**Policy VIIIA.1:** Separation of duties must be maintained when cash or cash equivalents are received. No single person should have complete control over the entire process of receiving, processing applying a payment, preparing the bank deposit and verifying the deposit of cash or cash equivalents.

**Policy VIIIA.1.1:** Tasks incompatible with cashiering shall not be performed by cashiers (e.g. collection follow-up of accounts receivable, distribution of pay warrants or other checks).

**Policy VIIIA.1.2:** The person collecting cash, issuing cash receipts, and preparing the departmental deposit shall be someone other than the person performing the monthly review of the General Ledger or the person maintaining accounts receivable records.

**Policy VIIIA.1.3:** Mail remittances must be verified as a payment to CSUF and then processed by a separate employee/individual. Mailed remittances shall be verified and processed by two employees. Mailed remittances must be restrictively endorsed for deposit or electronically deposited no later than by the close of business on the date of receipt.

**Policy VIIIA.2:** Individual accountability must be maintained and documented for all cash handling procedures:

**Policy VIIIA.2.1:** A unique identifier (Operator ID, user ID, login, password) not accessible or shared with other people shall be assigned to each cashier and/or individual in a department. A cash register drawer (aka cash fund), a cash drawer insert or another secure cash receptacle to which only the cashier has access will be provided. An individual endorsement stamp or its mechanical or electronic equivalent will be provided to allow for tracking of deposited and/or returned items back to the department and individual that/who accepted the items.

**Policy VIIIA.2.2:** Cashiers must lock all cash in a drawer or secure receptacle whenever leaving the immediate area.

**Policy VIIIA.2.3** Documentation of cash differences must be maintained for each cashier for subsequent review by a supervisor.

**Policy VIIIA.3:** All transfers of Cash and Cash Equivalents must be documented and the documentation of accountability maintained by category (i.e. currency, checks and other forms of payment).

### B. Receiving and Recording Cash and Cash Equivalents:

**Policy VIIIB.1:** In a timely manner, Checks and Cash Equivalents must be restrictively endorsed "for deposit only". All cash equivalents should be restrictively endorsed as soon as possible but no later than the close of business on the date of the receipt. Where electronic deposit is available and completed no later than by the close of the business on the date of receipt, then restrictive endorsement is not required.

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

- Policy VIII.B.1.1:** An individual endorsement stamp or its mechanical or electronic equivalent will be provided to allow for tracking of deposited and/or returned items back to the department and individual that/who accepted the items.
- Policy VIII.B.2:** An official CSUF cash receipt shall be recorded for each collection. A copy of the receipt shall be provided to payers making an in-person payment and to payers making currency and coin payments through the mail (common carrier). Although receipts shall be produced for check payments received through the mail, the mailing of a receipt to the payer is only required when the payer has requested a receipt.
- Policy VIII.B.3:** Under no circumstances will checks be routed to other offices to obtain recording information. When the proper account(s) to which a check should be credited cannot be readily determined, the check will be sent to the CSUF University Cashier. An uncleared collections cash received recording will be made and a copy of the check (in lieu of the check) will be distributed to appropriate offices for reference to determine the account distribution.
- Policy VIII.B.4:** Reductions of recorded cash accountability, e.g., voids and refunds, must be supported by all copies of the document involved, explained, and approved in writing/electronically by the cashier's supervisor at the time of occurrence where practical, but no later than the end of the day.
- Policy VIII.B.5:** A collection not recorded on cashiering software (CASHNet) must be recorded on an official pre-numbered, multiple parts Cash Receipt.
- Policy VIII.B.5.1:** The receipts must be numbered and issued in sequential order and be inventory-controlled.
- Policy VIII.B.5.2:** The form must include a statement that the form is recognized as a receipt only after validation by cashier's or cash handling employee's initials or signature, or by validation stamp to identify the cashier or cash handling employee recording the transaction.
- Policy VIII.B.5.3:** All voided receipts must be retained (i.e., not given to the customer) and have signed and/or electronic approval by a supervisor.
- Policy VIII.B.5.4:** Current day collections of Main Cashiering Stations must be deposited the same day, or at a minimum on the following business day.
- Policy VIII.B.5.5:** Collections at Satellite Stations and Departments must be deposited at the designated Main Cashiering Station or deposited with the bank directly the same day, or at a minimum on the following business day or whenever collections exceed \$500.
- Policy VIII.B.6:** Electronic Based Cashier Point-of-Sale (POS) Equipment (CASHNet) must meet CSUF's security and operational standards which are the following:

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

- Policy VIII.B.6.1:** All cash registers and Point-of-Sale (POS) equipment must produce a cash receipt with campus identifier for each customer.
- Policy VIII.B.6.2:** The equipment must have a feature for machine validation of cash-related documents.
- Policy VIII.B.6.3:** The cash-recording equipment must be controlled by unique consecutive numbers generated automatically and recorded with each transaction, as well as imprinted on the customer receipt.
- Policy VIII.B.6.4:** The numbering mechanism providing consecutive transaction number control must be accessible only to the manufacturer's service representative or appropriate personnel who are independent of that cashiering station.
- Policy VIII.B.6.5:** A unique identifier (Operator ID) that is not accessible to other people must be assigned to each cashier/remittance processor. A cash register drawer, cash drawer insert, and an endorsement stamp or its mechanical equivalent must also be provided.
- Policy VIII.B.7:** A Remittance Processor (Lockbox) must meet the security and operational procedures of CSUF, which are:
- Policy VIII.B.7.1:** The remittance system must provide a statement of activity, report, or electronic notification of activity to individual or department customers (i.e., post to student accounts).
- Policy VIII.B.7.2:** The remittance system must have a numbering validation system that provides consecutive transaction number control that is accessible only to the manufacturer's service representative, or appropriate personnel independent of that cashiering station.
- Policy VIII.B.7.3:** The remittance system must provide a unique identifier for each operator that is not accessible to others.
- Policy VIII.B.7.4:** The remittance system must endorse checks and verify individual cashier transactions.
- Policy VIII.B.7.5:** The remittance system must document all voided transactions.
- Policy VIII.B.7.6:** The remittance system must have security in place so that previous day's transactions cannot be altered.
- Policy VIII.B.8:** Checks drawn on foreign bank accounts that are not acceptable at face value by the depository bank must only be recorded as uncleared collections, and must be sent to an approved depository bank for collection. The Director (or Associate Director) of SFS may approve the use of alternate, fully documented, procedures for the handling and recording of checks drawn on foreign banks. Checks or equivalent financial instruments must be in United States Dollars.

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

### C. Point-of-Sale Equipment –Debit and Credit Card Processing

**Policy VIIIC.1:** Cashiering sites that accept MasterCard, Visa, American Express or Discover Card and PIN based Debit Card transactions will use only Point of Sale technology supplied to the location by the Campus' Merchant Card processor.

**Policy VIIIC.2:** All Point-of-Sale terminals, systems and cashiering sites must comply with the standards outlined in the Payment Card Industry Data Security Standards (PCI-DSS) and noted in Appendix B. PCI-DSS Data Security.

### D. Point of Purchase (POP) & Back Office Conversion (BOC) ACH Requirements

**Policy VIIID.1:** CSUF must comply with NACHA (National Automated Clearinghouse Association) established rules to support Standard Entry Class (SEC) transactions called the Point of Purchase (POP). Although Back Office Conversion (BOC) and Accounts Receivable Conversion (ARC) is established by NACHA, such transactions are not acceptable transactions or payments at CSUF.

In POP, a paper check is presented at the point of sale. The check is passed through an electronic check reader, which reads the Magnetic Ink Character Recognition (MICR) numbers at the bottom of the check [ABA routing and transit number, checking account number and check serial number]. The customer must sign the sales draft authorizing the electronic charge to his/her bank account. The check is then voided and returned to the customer with a copy of the sales draft receipt. The transaction is processed electronically and funds are withdrawn directly from the customer's checking account.

Subsection 3.8.1 of the National Automated Clearinghouse Association (NACHA) Operating Rules requires the following may not be used as source documents for POP entries: (1) checks drawn on corporate or business deposit accounts bearing auxiliary on-us numbers in the checking account number, (2) third-party checks, (3) credit card convenience checks, (4) obligations of a financial institution (e.g., traveler's checks aka traveler's cheques), cashier's checks, official checks, money orders, etc.), (5) checks drawn on the Treasury of the United States, a Federal Reserve Bank, or a Federal Home Loan Bank, (6) checks drawn on a state or local government, (7) checks payable in a medium other than United States currency or (8) eligible checks payable in excess of \$25,000.

### E. Sale of Admission or Event Tickets

**Policy VIIIE.1:** Sale of Admission or Event Tickets in person, procedures, standards and security must be equivalent to those stated in the Cash/Cash Equivalent Recording Sections (see Policy Section X).

**Policy VIIIE.2:** Tickets must be consecutively pre-numbered or produced by electronic means, when the numbering system is not accessible to ticket sellers.

Each ticket is considered both the product and the receipt. **All ticket sales must be balanced to their generated revenue on a daily basis.** When admission tickets or individual items are sold at the gates of athletic or other events, cashiering equipment may not always be present, nor may receipts be issued.

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

The Campus department/unit or Campus Merchant Card location selling tickets or other items must develop adequate controls to safeguard tickets, including the use of pre-numbered ticket stock, and cash collections and to ensure that the number of tickets or items sold corresponds to the expected revenue from the sale of the tickets or items. These controls must be reviewed by the Controller and/or Director (or Associate Director) of SFS maintained for audit purposes.

**Policy VIII.E.3:** A full accounting of “tickets sold” against cash received and amount posted to the General Ledger should be completed periodically to make certain that assets distributed at the point of sale are properly converted to cash and that the cash is being deposited into the cashier’s cash box.

### F. Credit/Debit Card Batch Processing (University of Extended Education ONLY)

**Policy VIII.E.1:** Paper-based authority received in the mail (common carrier) to charge a customer’s credit or debit card must use the following procedures:

- a) The authorization must be correctly executed/signed by the cardholder.
- b) The credit or debit card account number must be provided in combination with the expiration date.
- c) The authorization form must also include the correct billing address for the credit and/or debit card.
- d) The card information received in the written authorization is then to be manually input into the Merchant Card processing equipment supplied by the Merchant Card processor. Authorized codes are to be noted clearly on the authorization form received from the customer.
- e) All authorization forms that include customer account numbers and other personal information are to be stored with extreme care and accessible only to persons with appropriate authorities. Pursuant to card association rules, CSUF does not retain/store the CVV or customer PIN numbers beyond transaction authorization. It is advisable to store the data digitally, encrypt the data and grant access only to authorized persons with id and password protection. This encryption and password protection must comply with Payment Card Industry Data Security Standards (PCI-DSS) and follow data security noted in Appendix B of this document.

### G. Telephone

#### 1. Credit/Debit Card Processing (University of Extended Education ONLY)

CSUF does not accept or process Telephone Conversion (TEL) ACH-type transactions governed by NACHA. CSUF does not accept Credit and Debit card payments made over the telephone. University of Extended Education (“UEE”) does accept Credit and Debit card payment made over the phone. Such payments qualify for “*cardholder not present*” rules issued by the Credit Card Associations and mean that the ultimate risk of fraudulent payment instructions resides with the Merchant (in this case, UEE). The process works as follows:

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

**Policy VIII.G.1.1:** The Credit or Debit card account number and CVV or PIN number must be supplied during the telephone conversation in combination with the expiration date.

**Policy VIII.G.1.2:** The correct billing address for the Credit and/or Debit card must be obtained.

**Policy VIII.G.1.3:** The card information received in the telephone authorization is then to be manually input into the Merchant Card processing equipment supplied by the Merchant Card processor. Authorization codes are to be noted clearly on the form used to document the data obtained from the customer.

**Policy VIII.G.1.4:** All data collection forms that include customer account numbers and other personal information should be stored with extreme care and accessible only to persons with appropriate authorities. Pursuant to card association rules, do not retain/store the CVV or customer PIN numbers. It is advisable to store the data digitally, encrypt the data and grant access only to authorized persons with id and password protection. Please see [Purchase Card Industry \(PCI\) security standards](#) included in Appendix B.

### H. Prohibition on Payment with Credit/Debit Card via Fax Transmissions

#### 1. Credit/Debit Card Processing

**Policy VIII.H.1:** CSUF shall not accept payment instructions or cardholder information via fax transmission. This practice is prohibited as a violation of the intent of Section 4(a) of the Uniform Commercial Code (UCC).

### I. Payment with Credit-Debit Cards via the Internet

#### 1. Information Security

**Policy VIII.H.1.1:** CSUF accepts payments from customers over WEB-enabled connections facilitated by the Internet. CSUF subscribes to the Purchase Card Industry (PCI) Data Security Standards, known as PCI-DSS.

Any CSUF department/unit or Campus Merchant Card location using WEB-based payment methods (whether operating the system internally or through a third party) must comply with current PCI-DSS security standards on the PCI website and in Appendix B. PCI-DSS Data Security. PCI-DSS compliance is coordinated with the campus Information Security Officer and Director (or Associate Director) of SFS.

#### 2. Credit/Debit Card Gateway

**Policy VIII.H.2.1:** All CSUF deployed Gateways must operate in conformity with prevailing PCI Data Security Standards (PCI-DSS) and must be compatible with CSUF's Merchant Card processor. PCI-DSS

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

compliance is coordinated with the campus Information Security Officer and Student Financial Services Appropriate Administrator.

### 3. WEB ACH Transactions

**Policy VIIIH.3.1:** CSUF departments may use WEB ACH (aka: e-checks) at their Internet Gateways to allow customers to pay for goods and services by authorizing an ACH debit to their bank accounts. Any CSUF department/unit or Campus Merchant locations that deploys WEB ACH must use a CSUF approved service provider.

## IX. PHYSICAL SECURITY

CSUF has established procedures under ICSUAM 3102.04, Physical Protection of Cash and Cash Equivalents, and ICSUAM 3102.11, Deposits and Transfers to the Bank, to ensure physical security of cash and cash equivalents at all times. The campus CFO must establish campus-wide procedures to ensure the safety and security of deposits and personnel while in transit between campus locations. At a minimum, transport must be accomplished jointly by at least two employees.

**Policy IX.1:** All cash and cash equivalents shall be physically protected from loss at all times.

**Policy IX.2:** Excess cash must be removed from the cash register drawer during the business day and transferred to a secure cash handling area/vault (See Policy Section X).

**Policy IX.3:** At the close of business, all cash must be secured per Policy IX.6.

**Policy IX.4:** Deposits must be adequately protected from loss while in transit between campus locations. At a minimum, transport must be accomplished jointly by at least two employees. When deposits exceed \$2,500, employees shall be escorted by campus police. When determined necessary, armored car service or police protection should be used (armored car service to be arranged via the Associate Director of SFS.) Transporting deposits between cashiering sites or to the bank will be accomplished in a secure manner in order to protect the financial assets and individuals involved in transport.

**Policy IX.5:** Cash and cash equivalents must be locked in a secure receptacle or safe at all times except when signed out by a cashier for working cash.

**Policy IX.6:** Lockable receptacles or burglarproof/fire resistant safes to store cash and cash equivalents must be used on the following cash limits:

1. Up to \$1,000 in a lockable receptacle
2. From \$1,001 to \$2,500 in a safe
3. From \$2,501 to \$25,000 in a steel-door safe, with a door thickness of not less than 1 inch and wall thickness of not less than ½ inch
4. From \$25,001 to \$250,000 in a class TL-15 composite safe or better
5. Over \$250,000 in a class TL-30 steel or better safe

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

Deviation from these procedures may risk CSUF's loss of liability coverage with insurance carriers.

- Policy IX.7:** If more than \$2,500 in cash and cash equivalents is regularly on hand, a manual robbery alarm system or other appropriate measures must be installed at the location for use during business hours to alert Campus police (or the local police department for offsite locations) if an irregularity occurs.
- Policy IX.8:** If more than \$25,000 in cash and cash equivalents is stored, an automated alarm system is required to alert Campus police (or local police department for offsite locations) if the storage area is entered after business hours.
- Policy IX.9:** The safe's combination must be given only to supervisory and authorized personnel who must then commit the combination to memory. A record of the combination, sealed and open only under double-custody to prevent undetected access, must be maintained away from the safe area. The Department Manager/Supervisor is responsible for keeping a record of the named individuals who know the combination to the safe.
- Policy IX.10:** A safe must be opened in such a way that other persons do not view the combination.
- Policy IX.11:** To the maximum extent practical, a safe must be locked between uses during business hours.
- Policy IX.12:** A safe's combination must be changed whenever a person who knows the combination leaves the employ of a cash handling department or Campus Merchant Card processing location. Documentation (i.e. log) must be maintained showing the date and the reason for all safe combination changes. The Department Manager/Supervisor is responsible for coordinating, making and retaining the documentation of all safe combination changes.
- Policy IX.13:** Each cashier must be provided with a separate lockable box or compartment in the safe to which only that cashier has access. Duplicate keys must be safely stored away from the safe and be retrieved only under dual control.
- Policy IX.14:** Funds or property not related to the operation of CSUF must not be stored in the safe/vault.
- Policy IX.15:** The Director (or Associate Director) of SFS, together with the Campus Risk Management and University Police Departments, review the physical setup of cashiering stations to ensure that appropriate physical security is provided. As a general guideline, if a cashier station or Merchant Card Processing station collects more than \$7,500 on a daily basis, the work area should be protected by doors and windows that meet the standards of CSUF campus security standards. All University Main Cashiering Stations should record the handling and processing of cash and cash equivalents using surveillance cameras that capture actions in all areas of the Cashiering Station.
- Policy IX.16:** Campuses will develop and deliver Cash handling training to all Cash handling employees:

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

- **When a new employee commences work in a Cash handling job**
- **At least once per year for all Cash handling employees to refresh knowledge concerning policies, procedures and techniques and to provide updated information on internal and external policies**

Cash handling staff will also receive training on what to do in the event of a Campus emergency.

**Policy IX.17:** **Transporting deposits between cashiering sites or to the bank will be done in a secure manner in order to protect the financial assets and individuals involved in transport.**

**Policy IX.18:** **Satellite Cashiering Stations, Cash Handling Departments and Accounting Services & Financial Reporting Offices may transport cash and cash equivalents to a University Main Cashiering Station using the following methods:**

1. **By secure armored car service**
2. **By employees, in dual custody, transporting (walking or driving) the deposit to the University Cashier. In the case of cash deposits in excess of \$2,500, employees should be escorted by a Campus Security or University Police Officer.**

### X. RECORDING DEPOSITS TO THE GENERAL LEDGER

Per ICSUAM 3102.08, Recording Deposits to the General Ledger, and monthly reconciliation of deposit records must be performed to ensure that all deposits are deposited into a University depository account and properly recorded on the general ledger in an accurate and timely manner. The deposits and transfers recorded in the General Ledger are governed by ICSUAM 3102.11, Deposits and Transfers to the Bank as well as 3101.02, Campus Administration of Systemwide Cash Management.

**Policy X.1:** **Deposits to banks must be reviewed, approved and recorded to the General Ledger in a timely manner.**

**Policy X.2:** **All bank deposits must be accounted and recorded into the General Ledger during the appropriate month by Accounting Services & Financial Reporting staff and/or management.**

Accounting Services & Financial Reporting shall receive the bank statements directly from the bank and retain them until the reconciliations are completed.

Monthly bank reconciliations must be completed within 30 days of the preceding month and must show the preparer's name/signature, reviewer's name/signature, date prepared, and date reviewed. Discrepancies between the general ledger cash balances and closing balances on bank statements shall be investigated independently by Accounting Services & Financial Reporting management.

**Policy X.3:** **Individuals with cash handling responsibilities may not prepare and post journal entries.**

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

- Policy X.4:** All journal automatic and manual entries must be reviewed and approved by designated employees in the Accounting Services & Financial Reporting Services Office. The preparer and reviewer/approver must be different persons.
- Policy X.5:** Processing incoming Wire Transfers and ACH Payments
- Wire Transfer and ACH credit transactions must be accessed through the bank's balance and transaction reporting system and recognized in the General Ledger each business day.
  - Recording to the appropriate General Ledger and/or Receivable accounts must occur within two working days. All unidentified deposits will be posted to a specific "uncleared collections" account.
  - A unique identifier must be applied to the credits of an individual day's work, so the credits can be traced back to the correct deposit date. All funds received on a specific date must be applied in total for that date.
  - A method of identifying and tracing funds in the specific "uncleared collections" must be in place.
  - Separation of duties – the employee capturing and crediting the funds cannot reconcile the bank statements.

### XI. RETURNED ITEM PROCESSING

#### A. Cash Equivalents (non-coin & currency) and Checks

As governed by ICSUAM 3102.06, Returned Items, cash equivalents may be returned unpaid by the banking system for a number of reasons but the primary cause of returned Cash Equivalents is counterfeiting or lost/stolen instruments that have been stop-paid. Cash Equivalents returned to the Campus must be controlled during the process of attempting to collect on the returned amount. Student Accounts in SFS, a non-cashiering area, is to provide oversight over the returned cash equivalent process.

Checks may be returned unpaid by the banking system for a number of reasons; the primary causes of returns are non-sufficient funds, account closed and stop payment. Checks returned to the Campus must be controlled during the process of attempting to collect on the returned amount. Student Accounts in SFS, a non-cashiering area provides oversight over the returned check process.

- Policy XIA.1:** Cash Equivalents that are deemed to be uncollectible are to be returned by the depository bank to the designated non-cashiering department (SFS Student Accounts)
- Policy XIA.2:** Cash Handlers must not be involved in the returned Cash Equivalent process
- Policy XIA.3:** The person who approves the request for write-off of uncollectible cash equivalents must not maintain the inventory of returned cash equivalents
- Policy XIA.4:** A returned cash equivalent must be redeemed by a new payment
- Policy XIA.5:** The person maintaining the inventory of returned cash equivalents must not handle the cash received to redeem returned cash equivalents

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

**Policy XIA.6:** No one person from the same office may perform more than one of the above functions (Policy Sections XIA.2-XIA.5)

**Policy XIA.7:** Physical security and accountability for returned Cash Equivalents must be maintained from the time of receipt of the returned item until final disposition

### B. ACH Debit Transactions

ACH debit transactions may be rejected by the banking system for a number of reasons; the primary causes of returned debits are incorrect account information, non-sufficient funds, account closed, no authorization or authorization revoked. ACH debits returned to the Campus must be controlled during the process of attempting to collect on the returned amount. SFS Student Accounts area provides oversight over the returned ACH debit process.

**Policy XIB.1:** ACH debits that are deemed to be uncollectible are to be returned by the Originating Financial Depository Institution (depository bank) to the designated non-cashiering department, SFS Student Accounts or Accounting Services & Financial Reporting.

**Policy XIB.2:** Cashiers must not be involved in the returned ACH debit process.

**Policy XIB.3:** The person who approves the requests for write-off of uncollectible ACH debits must not maintain the inventory of returned ACH debits.

**Policy XIB.4:** A returned ACH debit must be redeemed by a new payment.

**Policy XIB.5:** The person maintaining the inventory of returned ACH debits must not handle the cash received to redeem returned ACH debit.

**Policy XIB.6:** No one person from the same office may perform more than one of the above functions (Policy Sections XIB.2-XIB.5).

### C. Credit/Debit Card Chargebacks

Credit and Debit Card returns, also known as chargebacks, are the consequence of:

1. Unauthorized/fraudulent use of a credit or debit card
2. An unresolved dispute between the payer and CSUF:
  - a. The payer argues that a good or service was not received
  - b. The payer argues that a good or service was not received as promised (i.e. product or service failure)
  - c. The payer argues that the Merchant (CSUF) overcharged for the good or service.

CSUF will be notified that the cardholders' (payer's) bank intends to process a chargeback to the Campus prior to the actual debit transaction. This "courtesy" is extended to all Merchants to permit the Merchant to "dispute" the chargeback, so these notifications should be researched and responded to upon receipt. Chargebacks are debited by CSUF's Merchant Card processor to the Campus Merchant Card Account. The chargeback will identify the Merchant ID (which translates to a specific Campus business department)

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

that accepted the payment and that Merchant ID will be debited for the returned item. The Director or Associate Director of SFS or their designee is to notify the affected business department of all chargebacks both during the courtesy notification period as well as when a chargeback is actually received.

- Policy XIC.1:** Credit/Debit card chargebacks are to be returned by the Merchant Card processor to the designated non- cashiering department
- Policy XIC.2:** Cashiers must not be involved in the returned Credit/Debit Card chargeback
- Policy XIC.3:** The person who approves the requests for write-off of uncollectible Credit/Debit Card chargebacks must not maintain the inventory of returned Credit/Debit Card chargebacks
- Policy XIC.4:** A returned Credit/Debit Card chargeback must be redeemed by a new payment
- Policy XIC.5:** The person maintaining the inventory of returned Credit/Debit Card chargebacks must not handle the cash received to redeem returned Credit/Debit Card chargebacks
- Policy XIC.6:** No one person from the same office may perform more than one of the above functions (Policy XIC.2-XIC.5)

### XII. CONTRACTING WITH THIRD PARTY RELATIONSHIPS TO PROCESS CASH AND CASH EQUIVALENTS (INCLUDES LOCKBOX SERVICES)

CSUF may need contract with a third party to assist in the processing and management of cash, cash equivalents and ACH transactions. Third parties may provide to CSUF:

- Lockbox services
- Web/Internet interfaces to internal and external clients
- Processing of currency, coin and other cash equivalents
- Processing of electronic payments, particularly ACH entries
- Credit, Debit and Proprietary Card processing.

Relying on third parties to process the campus's Cash, Cash Equivalents and ACH transactions requires the CSUF campus to take extreme care in their selection and on-going management. Accordingly, the following policies are necessary to safeguard CSUF assets:

- Policy XII.1:** Campus CFO or designee must approve the use of any third party relationship where the third party is in possession of CSUF assets to process CSUF Cash, Cash Equivalents and/or ACH transactions and related processes
- Policy XII.2:** Before entering into any relationship with a third party, CSUF must have CSU CO Treasury Department perform an adequate review of the Third Party's background, capabilities, financial condition and references

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

**Policy XII.3:** Third Parties that assist CSUF with management of Cash and Cash Equivalents must enter into a CSUF approved contract that requires, at a minimum, the same level of protection, regulatory compliance (including, but not limited to Purchase Card Industry [PCI] Data Security Standards (PCI-DSS) and State of California Information Practice Act (Senate Bill 1386, privacy requirements), insurance, bonding, and accurate/timely handling of cash, cash equivalents and/or ACH transactions and Data as is established for CSUF by this document. CSUF is to be named as the sole loss-payee on any insurance and/or bonding agreements with third parties. All insurance carriers that provide protections to CSUF under Third Party Agreements (TPAs) must be approved by the CSU Chancellor's Office

**Policy XII.4:** Campus CFO must periodically review and affirm rational for 3<sup>rd</sup> party retaining CSU's cash "for longer than one business day".

### XIII. PETTY CASH AND CHANGE FUNDS

Petty Cash and Change Funds are governed by ICSUAM 3102.10, Change Funds, and ICSUAM 3103.11, Petty Cash. This Document Section also includes references to CSUF's Petty Cash & Change Fund policy, <http://finance.fullerton.edu/Controller/Accounting/PettyCash/>.

**Policy XIII.1:** Petty cash and change funds are provided as a service to operating departments that require such operating funds. Campus policies must be established to appropriately protect these funds from loss through the provision of safes, vaults or money chests. Requests to establish these funds are reviewed by the Controller.

**Policy XIII.2:** Petty cash funds must be separately maintained from cashier change funds.

#### 1. Authorization

Under ICSUAM Sections [3102.10](#), Change Funds, and [3103.11](#), Petty Cash, the campus CFO or his/her delegate may authorize establishment of petty cash/change funds at department offices or other approved locations. Requests/authorization for such funds must be documented in writing.

#### 2. To Establish a New Change Fund or Petty Cash Fund

A request to establish or increase a change fund or cash purchase fund must be made in writing by an authorized departmental staff person, such as the designated custodian or department head. The request shall be addressed to the Accounting Officer and shall contain the requested amount, the reason for the request, the assurance that the funds will be safeguarded and the name of the custodian of the funds. The Accounting Officer will review the request and, if approved, will prepare an Approving Memo that the custodian will sign, signifying understanding and approval of the regulations governing the maintenance of the fund. The check will then be issued to the name of the Custodian of the fund.

#### 3. To Decrease or Close a Change Fund or Petty Cash Fund

If a decrease in an existing fund is determined or to close a change fund or petty cash fund, notify Accounting Services & Financial Reporting. An unannounced final cash count will be done by the Director of Internal Audit as soon as Accounting Services & Financial Reporting is notified.

The fund will be balanced. After the final audit, the custodian of the fund must take the cash equal to the desired decrease or the full amount of the fund to the University Cashiers Office (UH-180). Complete the [Deposit or Reimbursement to University Account](#) form prior to making the cash deposit. On the form, use CASHNet item code S4000. This will credit account 580093 (Other Non-operating

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

Revenues). Once the deposit is made, submit an [Expenditure Transfer Request](#) form to reclassify from account 580093 to 101009 (Cash on Hand). Attach a copy of the receipt issued by the Cashier.

**Policy XIII.3:** Cash handlers must not exchange checks for currency to make change for each other. Any such change-making must be handled only by the custodian of the change fund.

### 1. Custodianship

Custodianship of a given fund should be assigned to a single individual. The custodian will be personally responsible for the amount of the fund.

To obtain replenishment of the fund, submit an [Accounts Payable Check Request](#) form with the appropriate original receipts per transaction. Check requests are payable to the custodian only.

The petty cash fund will be closed upon termination or departmental transfer of the custodian. Transfer of funds to a successor is not authorized. To change custodians, complete and submit the [Custodian Transfer Request – Change/Petty Cash Funds](#) form. This form must be completed prior to the departure of the relieved custodian. Keep a copy of the signed form and forward the original to Accounting Services & Financial Reporting.

**Policy XIII.4:** An unannounced cash count and reconciliation of change and petty cash funds for which cashiers and cash handling employees are accountable shall be performed on a periodic basis based on the amount in the fund (monthly or quarterly), by someone other than the fund custodian. Cash counts will be performed by the Director of Internal Audit or designee. Reconciliation of cash balances must be performed in the presence of the petty cash/change fund custodian and must be documented and maintained on file.

### Audit Requirements

All change funds and petty cash funds must undergo an independent unannounced audit (cash count and reconciliation) in accordance with the following schedule:

<u>Size of Fund</u>	<u>Frequency of Count</u>
<u>\$200.00 or less</u>	<u>Annually</u>
<u>\$200.01 to \$500.00</u>	<u>Quarterly</u>
<u>\$500.01 and over</u>	<u>Monthly</u>

These audits will be performed by Director of Internal Audit or their staff, in the presence of the custodian of the fund. The Petty Cash Fund Audit and Change Fund Audit Forms will be completed at the time of the audit by the auditor of the funds and will be signed by the custodian and the auditor. A copy of this form will be given to the custodian at the conclusion of the audit. Any irregularities will be discussed and noted. A copy of the audit results will be submitted to the Accounting Officer for review and will be retained.

### 1. Additional Internal Controls for Petty Cash Funds

Petty cash funds represent idle funds which validate an ongoing need for additional security, record-keeping, and audit. The below items support the additional internal controls required for petty cash funds maintained by the campus community.

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

- Petty cash funds shall maintain the established dollar value. No petty cash fund shall be established with an amount exceeding \$500 except with prior approval of Accounting Services & Financial Reporting and the University Controller.
- Individual petty cash transactions must be supported by proper documentation of the original transaction. Each petty cash voucher must be accompanied by an original receipt upon reimbursement or return of unused funds. A signature and printed name is required on each voucher. The voucher is to remain as permanent document of the fund's transactions and retained by the custodian until closure. Splitting a transaction into multiple reimbursements is not allowed
- Petty cash disbursements may not be held for future use by any employee for an excessive period.
- Reimbursements to the petty cash fund are to be submitted to Financial Services in sufficient time to prevent depletion of the fund. All check payments processed for reimbursement by Accounts Payable shall be made payable to the institution or custodian and directly reference the fund
- Any discrepancy in petty cash funds shall be the personal responsibility and liability of the custodian(s)
- Any petty cash funds found to be misappropriated or out of balance without cause will be immediately closed and appropriate action will be taken
- The petty cash fund must be maintained in a locked, secure location at all times
- Petty cash funds are to be used for business purposes only. Petty cash funds must never be commingled with personal or other funds
- Under no circumstance shall petty cash funds be deposited in a personal bank account
- When petty cash/change fund is no longer needed, petty cash/change funds will be re-deposited at the cashiering office
- The custodian shall balance petty cash funds after each payment. The fund shall be balanced at least weekly by the custodian regardless of use
- If the petty cash fund has not been used for three fiscal quarters it must be closed. Accounting Services & Financial Reporting will notify the custodian about possible closure from lack of use. If requested to be closed any date extensions beyond the original anticipated closure date must be in writing to Accounting Services & Financial Reporting and the University Controller. Such a request will require a review under the same procedures as its original establishment of the petty cash fund

### **2. Theft of Petty Cash Funds**

In the event of theft, notify Campus Police immediately. A new request should be submitted requesting reimbursement of the fund which includes the following:

- Date and time of theft
- Amount of theft
- Circumstances involved
- Copy of police report
- Prevention taken against similar occurrences

### **3. Petty Cash Funds Types of Expenditures & Transaction Requirements**

Expenses that cannot be paid from petty cash include, but are not limited to, the following: invoices from vendors, payments for services to employees or independent contractors, loans and advances.

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

### APPENDIX A: GENERAL INFORMATION

#### **Credit and Debit Card Information**

**Cardholder Present:** This is a sale/payment condition where the buyer/payer is physically on site with his/her credit or debit card available for “swiping” through the credit/debit card terminal made available to the department by CSUF’s Merchant Card processor. This transaction is completed when the buyer’s/payer’s credit/debit card issuer authorizes settlement of the transaction and the buyer/payer has signed the credit/debit card transaction receipt. It is the cash handling department’s obligation to check the authenticity of the signature by comparing the signature on the receipt to the signature on the back of the credit card. If the credit card has not been signed then, and only then, can the cash handling department ask to see the buyer’s/payer’s driver’s license.

The *Cardholder Present* model is beneficial to CSUF since it gives rise to the lowest discount rate from the Merchant Card Processor on the presumption that there will be lower rates of fraud and fewer chargebacks.

**Cardholder Not Present:** This is a sale/payment condition where the buyer/payer is not physically on site with his/her credit or debit card and, therefore, the cash handling department has collected the cardholder data (card number, name, expiration date, billing address) by telephone, or by WEB site. This transaction is completed when the buyer/payer provides the needed information to UEE via a telephone, or WEB site and CSUF then presents that data to the Merchant Card processor which obtains an approval or rejection message from the buyer’s/payer’s credit card issuer.

The *Cardholder Not Present* model is efficient and allows transactions to be completed when the buyer/payer is not physically on site but it does give rise to a higher discount rate from the Merchant Card Processor on the presumption that there will be higher rates of fraud and more chargebacks. Additionally, in most cases, the merchant site accepting payments in the *Cardholder Not Present* model typically must absorb any and all losses that arise from fraud or customer initiated chargebacks.

#### **Detecting Counterfeit Money**

Adopted from the United States Secret Service

CSUF has a role in maintaining the integrity of U.S. currency. Campus personnel can help guard against the threat from counterfeiters by becoming more familiar with U.S. currency. Campus personnel should examine the money received closely. They should compare a suspect note with a genuine note of the same denomination and series, paying attention to the quality of printing and paper. Personnel should look for differences, not similarities.

If a counterfeit note is received:

1. Do not return it to the passer.
2. Defray the passer if possible.
3. Observe the passer's description, as well as that of any companions, and the license plate number of any vehicles used.
4. The cashier should write his/her initials and the date in the white border areas of the suspect note.
5. Limit the handling of the note. Carefully place it in a protective covering, such as an envelope.
6. Forward the note to University Cashier site or surrender the currency or coin only to a Campus Police Officer or a U.S. Secret Service Special Agent. If received in the University Main or Satellite Cash Handling site, forward the note directly to the U.S. Secret Service. The note should be forwarded following campus procedures. The U.S. Secret Service field office will normally mail the note back to the campus if it is not a counterfeit note or will send a letter indicating that it is a counterfeit note.

For more information on how to detect counterfeit money consult the U. S. Secret Service website, *Know Your Money*, [http://www.secretservice.gov/know\\_your\\_money.shtml](http://www.secretservice.gov/know_your_money.shtml).

#### **Reason Codes for why Payment Types may be Returned**

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

The following chart highlights the primary reasons for return of each payment types in the left hand column. For instance, every payment type, except ACH, can be returned to the depositor if the entry was deemed to be counterfeit.

	Counterfeit/ Altered Item	Non- Sufficient Funds	Stop Paid	Stale Dated	Account Closed	Fraudulent Endorsement	Not- Authorized	Product or Service Dispute
Cash	X							
Cash Equivalents	X		X	X		X		
Checks	X	X	X	X	X	X		
ACH		X			X		X	
Credit/ Debit Cards	X						X	X

### Time Limits by which Payment Types Must Legally be Returned

	Counterfeit	Non- Sufficient Funds	Stop Paid	Stale Dated	Account Closed	Fraudulent Endorsement	Not- Authorized	Product or Service Dispute
Cash	Days							
Cash Equivalents	24 hour reclamation		24 hour reclamation	24 hour reclamation		90 days		
Checks	24 hour reclamation	24 hour reclamation	24 hour reclamation	24 hour reclamation	24 hour reclamation	90 days		
ACH		24 hour reclamation			24 hour reclamation		60 days	
Credit/ Debit Cards	60 days						60 days	60 days

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

### APPENDIX B: PCI-DSS DATA SECURITY

Protection of CSUF assets and technology resources that support CSUF's operation is critical to the functioning of CSUF. CSUF information assets are at risk from employee error, malicious or criminal action, system failure, natural disasters, etc. Such events could result in damage to or loss of information resources, corruption or loss of data integrity, interruption of the activities of CSUF, or compromise to confidentiality or privacy of members of CSUF campus community.

CSUF Cashiering functions routinely process highly sensitive data both in paper and electronic form. Accordingly, it is critical that all Cashiering locations process and store sensitive data with utmost care to protect the privacy of CSUF constituencies and avoid any financial losses that may arise from the unauthorized use or disclosure of confidential information.

CSUF has issued data retention and security policies for both electronic and paper media. Accordingly, this document refers each CSUF Cashiering site to the following policy statements for general guidance concerning the receipt, handling, storage and retention of private, restricted data:

Refer to [Senate Bill 1386](#) for privacy requirements.

Specific Data Security guidelines for CSUF Cashiering sites:

1. The privacy and confidentiality of all accessible data is to be maintained and it is understood that unauthorized disclosure of personal/confidential information is an invasion of privacy, may be illegal, and may result in disciplinary, civil and/or criminal actions against an individual.
2. Training in data security must be provided by each Campus to any user of highly secure information, especially private information, related to management, use, and protection. This training may be overarching, or specific (such as FERPA training for student data).
3. Systems should not include restricted information unless it is absolutely necessary.
4. Restricted data elements, such as Social Security Number, ethnicity, date of birth and financial information such as credit card number or bank account number, should never be used as the 'key' to a system.
5. Do not download restricted data from a database system to your laptop or desktop unless there is an unavoidable business need. If this information is downloaded, ensure that it is protected against hacking or loss (for instance encryption), and that it is removed as soon as possible.
6. Do not e-mail restricted data, either in the body of an e-mail or as an attachment.
7. Encrypt restricted data in storage. Protect the encryption key from unauthorized disclosure.
8. Credit card account and transaction information must not be sent via unencrypted e-mail messages over the Internet. CSUF subscribes to the Payment Card Industry (PCI) Data Security Standards
9. Require Secure Sockets Layer (SSL) protocol for all credit card account and transaction information transmitted over the Internet.
10. Never store payment data on a web server or cache anywhere in memory related to a web server. Payment data may only be stored in a separate, secure database, with at least one external firewall.
11. Ensure that critical data is backed up and that a business resumption plan exists and that backed up data is stored in a secure manner.

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

---

### **System and Data Access**

1. Access to the system should only be given to individuals when it is necessary to perform their job duties, and the “process owner” should approve any access granted.
2. Restrict physical access to student payment and personal data.
3. Restrict physical entry to e-commerce web servers to authorized personnel.
4. An individual’s access should be deleted immediately when their job duties no longer require that access. A listing of individuals with systems access should be reviewed at least annually by the “process owner” to ensure that only authorized individuals have access.
5. Assign a unique ID to each person with computer access to payment data.
6. Maintain the ability to track employee access to payment data through the use of unique IDs.
7. Do not share passwords. Restrict access to information based on a ‘need to know’ basis. Lock your computer when not in use. Set-up computers to time out and require sign in when not used for a reasonable amount of time. When you print restricted paper, pick it up immediately and shred when finished.
8. Change employee passwords regularly.

## CSUF CASH MANAGEMENT POLICY

Updated: July 1, 2014

### APPENDIX C: ICSUAM 3101.02 - ANNUAL COMPLIANCE REVIEW CHECKLIST

#### California State University, Fullerton CASH MANAGEMENT PLAN ANNUAL REVIEW CHECKLIST

**Fiscal Year:** \_\_\_\_\_

Required by CSU ICSUAM 3101.02, Campus Administration of Systemwide Cash Management Policy, the campus CFO or his/her delegate must ensure that an annual documented review of compliance with these policies and procedures is performed with risk results reported to the campus CFO. The below checklist is such documentation.

INITIALS	ICSUAM CASH MANAGEMENT 3101.02	COMMENTS
	Reviewed the designation of cash handling units and individuals/positions performing functions related to cash handling and cash accounting.	
	Reviewed the process for creating or dismantling approved cashiering/ sub-cashiering locations, including physical locations, websites, 3rd party processors, or any channel accepting credit card payments.	
	Performed review to ensure that the person or persons properly authorized to sign checks, drafts, or other orders for payment of money or to approve/release electronic transfers of funds against CSU checking accounts is/are covered by a fidelity bond.	
	Monthly bank reconciliations must be completed within 30 days of the preceding month and must show the preparer's name/signature, reviewer's name/signature, date prepared, and date reviewed. Discrepancies between the general ledger cash balances and closing balances on bank statements shall be investigated independently by Accounting Services and Financial Reporting management.	
	Cash collections over \$200,000 must be reported via telephone or email to the Chancellor's Office Treasury Department the day of collection to facilitate centralized cash management.	
	Trained, upon employment, or retrained all cash handling employees on their cash handling role, procedures and responsibilities annually. Training content includes cash handling procedures during a campus emergency. Employees in positions where cash handling is not their primary duty are informed of designated cashiering sites and how to handle cash or cash equivalents that may be received at a non-cashiering location.	
	Reviewed the current Cash Management guideline to ensure compliance with applicable ICSUAMs, along with Federal, State and local authorities and campus policies and procedures.	

Preparer: \_\_\_\_\_  
University Tax Compliance Manager
Date

Reviewer: \_\_\_\_\_  
University Controller
Date